Communication Theory of Secrecy Systems (C. E. Shannon, 1949)
A Mathematical Theory of Cryptography (C. E. Shannon, 1946)

Claude Elwood Shannon (1916 - 2001)
The Father of Information Theory

Boolean Theory
- A Symbolic Analysis of Relay and Switching Circuits (1937)
- An Algebra for Theoretical Genetics (1940)

Cryptography
- A Mathematical Theory of Cryptography (1946)
- Communication Theory of Secrecy Systems (1949)

Information Theory
- A Mathematical Theory of Communication (1948)
Secrecy Systems

- Schematic of A General Secrecy System
  - $E = f(M, K)$
  - $E = T_i M$

![Schematic of a general secrecy system](image)

**Fig. 1. Schematic of a general secrecy system**

- Definition of Secrecy Systems
  - A Secrecy System is a family of uniquely reversible transformations $T_i$ of a set of possible messages into a set of cryptograms, the transformation $T_i$ having an associated probability $p_i$.
  - A set of transformations with associated probabilities
  - Domain and Range
  - More on the definition
- Threat Model
  - The enemy knows the system being used. (Shannon’ Maxim)
    - Objection

- Deciphering vs Cryptanalysis

- Representation of Secrecy Systems
  - Line diagram

\[\text{Fig. 2. Line drawings for simple systems}\]

- Closed system
Examples of Secrecy Systems

● Substitution
  ○ Simple Substitution
    ■ Key
    ■ wk lv phvvdjh lv qr w r wr kdg wr euhdn
  ○ Vigenère
    ■ Degree
    ■ \( e_i = m_i + k_i \pmod{26} \)

● Transposition
  ○ Columnar Transposition

● Combination

● One-time Pads
  ○ Unbreakable if used correctly / Information-theoretically secure
    ■ Perfect Secrecy
  ○ Problems
    ■ True randomness
    ■ Key size
    ■ Synchronization
  ○ Vernam Cipher
Characteristics of a Good Cryptosystem

- Shannon’s Criteria
  - Amount of Secrecy
    - Perfect
    - Not Perfect but never yield unique solution
    - Not Perfect and yield unique solution, but the amount of effort varies
  - Size of Key
  - Complexity of Enciphering and Deciphering Operations
  - Propagation of Errors
  - Expansion of Messages

- Are these criteria still reasonable?

- Anything else?
Mathematical Structure of Secrecy Systems

- Secrecy System

- Combination
  - Weighted Sum
  - Product

- Properties
  - Associative?
  - Distributive?
  - Commutative?
  - Endomorphic?
Pure Cipher

- Homogenenity
  - Group property

- Unrefined Defination
  - $T$ forms a group
  - Endomorphic

- Proper Definination
  - A cipher $T$ is pure if for every $T_i, T_j, T_k$ there is a $T_s$ such that $T_i T_j^{-1} T_k = T_s$, and every key is equally likely. Otherwise the cipher is mixed.

- Property
  - Theorem 1
  - Theorem 2
  - Theorem 3
  - Theorem 4
Perfect Secrecy

- Questions:
  - How immune a system is when the cryptanalyst has unlimited time and manpower available for the analysis of cryptograms?

- Natural Definition of Perfect Secrecy
  - It is natural to define perfect secrecy by the condition that, for all $E$ the a posteriori probabilities are equal to the a priori probabilities independent of the value of these.

- Theorem 6
  - A necessary and sufficient condition for perfect secrecy is that $P_M(E) = P(E)$ for all $M$ and $E$. That is, $P_M(E)$ must be independent of $M$.

- Important relationship between keys and messages
General Idea of Ideal Secrecy

- Problem with Perfect Secrecy
  - Key size

- Entropy and Equivocation
  - $H(M)$ and $H(K)$
  - $H_E(M)$ and $H_E(K)$

- Properties of Equivocation

- Definition of Ideal Secrecy
  - Ideal secrecy
    - $H_E(M)$ and $H_E(K)$ do not approach zero as $N \to \infty$.
  - Strongly ideal secrecy
    - $H_E(K)$ remains constant at $H_E(M)$. 